The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
AlstraSoft -- Video Share Enterprise	PHP remote file inclusion vulnerability in myajaxphp.php in AlstraSoft Video Share Enterprise allows remote attackers to execute arbitrary PHP code via a URL in the config[BASE_DIR] parameter.	unknown 2006-08-29	7.0	CVE-2006-4443 BUGTRAQ BID
Ay System Solutions -- Ay System Solutions CMS	PHP remote file inclusion vulnerability in main.php in Ay System Solutions CMS 2.6 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the path[ShowProcessHandle] parameter.	unknown 2006-08-29	7.0	CVE-2006-4440 OTHER-REF SECUNIA
Ay System Solutions -- Ay System Solutions CMS	Multiple PHP remote file inclusion vulnerabilities in Ay System Solutions CMS 2.6 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the path[ShowProcessHandle] parameter to (1) home.php or (2) impressum.php. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-08-29	7.0	CVE-2006-4441 SECUNIA
BigACE -- BigACE	Multiple PHP remote file inclusion vulnerabilities in Bigace 1.8.2 allow remote attackers to execute arbitrary PHP code via a URL in the (1) GLOBALS[_BIGACE][DIR][admin] parameter in (a) system/command/admin.cmd.php, (b) admin/include/upload_form.php, and (c) admin/include/item_main.php; and the (2) GLOBALS[_BIGACE][DIR][libs] parameter in (d) system/command/admin.cmd.php and (e) system/command/download.cmd.php.	unknown 2006-08-28	7.0	CVE-2006-4423 BUGTRAQ BID SECTRACK XF
CJ Design -- CJ Tag Board	Direct static code injection vulnerability in CJ Tag Board 3.0 allows remote attackers to execute arbitrary PHP code via the (1) User-Agent HTTP header in tag.php, which is executed by all.php, and (2) the banned parameter in admin_index.php.	2006-08-25 2006-08-29	7.0	CVE-2006-4451 OTHER-REF BID FRSIRT SECUNIA
CutePHP -- CuteNews	** DISPUTED ** Multiple PHP remote file inclusion vulnerabilities in CuteNews 1.3.x allow remote attackers to execute arbitrary PHP code via a URL in the cutepath parameter to (1) show_news.php or (2) search.php. NOTE: CVE analysis as of 20060829 has not identified any scenarios in which these vectors could result in remote file inclusion.	unknown 2006-08-29	7.0	CVE-2006-4445 BUGTRAQ MLIST BUGTRAQ XF
ExBB -- ExBB Italia	PHP remote file inclusion vulnerability in modules/userstop/userstop.php in ExBB Italia 0.2 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the exbb[home_path] parameter.	unknown 2006-08-31	7.0	CVE-2006-4488 OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF
Gonafish.com -- LinksCaffe	Gonafish.com LinksCaffe 2.0 and 3.0 do not properly restrict access to administrator functions, which allows remote attackers to gain full administration rights via a direct request to Admin/admin1953.php.	unknown 2006-08-31	10.0	CVE-2006-4462 BUGTRAQ
gtetrinet -- gtetrinet	Array index error in tetrinet.c in gtetrinet 0.7.8 and earlier allows remote attackers to execute arbitrary code via a packet specifying a negative number of players, which is used as an array index.	unknown 2006-08-31	7.0	CVE-2006-3125 DEBIAN
IBM -- AIX	Untrusted search path vulnerability in the mkvg command in IBM AIX 5.2 and 5.3 allows local users to gain privileges by modifying the path to point to a malicious (1) chdev, (2) mkboot, (3) varyonvg, or (4) varyoffvg program.	unknown 2006-08-28	7.0	CVE-2006-4416 AIXAPAR AIXAPAR BID SECUNIA

Jetbox -- Jetbox CMS	PHP remote file inclusion vulnerability in includes/phpdig/libs/search_function.php in Jetbox CMS 2.1 allows remote attackers to execute arbitrary PHP code via a URL in the relative_script_path parameter, a different vector than CVE-2006-2270. NOTE: this issue has been disputed, and as of 20060830, CVE analysis concurs with the dispute. In addition, it is likely that the vulnerability is actually in a third party module, phpDig 1.8.8.	unknown 2006-08-28	7.0	CVE-2006-4422 BUGTRAQ BID BUGTRAQ BUGTRAQ MLIST MLIST XF
Joomla! -- Joomla!	Unspecified vulnerability in PEAR.php in Joomla! before 1.0.11 allows remote attackers to perform "remote execution," related to "Injection Flaws."	unknown 2006-08-31	7.0	CVE-2006-4469 OTHER-REF
Joomla! -- Joomla!	Joomla! before 1.0.11 omits some checks for whether _VALID_MOS is defined, which allows attackers to have an unknown impact, possibly resulting in PHP remote file inclusion.	unknown 2006-08-31	7.0	CVE-2006-4470 OTHER-REF
Joomla! -- Joomla!	The Admin Upload Image functionality in Joomla! before 1.0.11 allows remote authenticated users to upload files outside of the /images/stories/ directory via unspecified vectors.	unknown 2006-08-31	7.0	CVE-2006-4471 OTHER-REF
Joomla! -- Joomla!	Multiple unspecified vulnerabilities in Joomla! before 1.0.11 allow attackers to bypass user authentication via unknown vectors involving the (1) do_pdf command and the (2) emailform com_content task.	unknown 2006-08-31	7.0	CVE-2006-4472 OTHER-REF
Joomla! -- Joomla!	Multiple cross-site scripting (XSS) vulnerabilities in Joomla! before 1.0.11 allow remote attackers to inject arbitrary web script or HTML via unspecified parameters in (1) Admin Module Manager, (2) Admin Help, and (3) Search.	unknown 2006-08-31	7.0	CVE-2006-4474 OTHER-REF
Joomla! -- Joomla!	Joomla! before 1.0.11 does not limit access to the Admin Popups functionality, which has unknown impact and attack vectors.	unknown 2006-08-31	7.0	CVE-2006-4475 OTHER-REF
Jupiter CMS -- Jupiter CMS	** DISPUTED ** PHP remote file inclusion vulnerability in index.php in Jupiter CMS 1.1.5 allows remote attackers to execute arbitrary PHP code via a URL in the template parameter. NOTE: CVE disputes this claim, since the $template variable is defined as a static value before it is referenced in an include statement.	unknown 2006-08-28	7.0	CVE-2006-4428 BUGTRAQ MLIST BID
Microsoft -- Terminal Server	** DISPUTED ** Microsoft Terminal Server, when running an application session with the "Start program at logon" and "Override settings from user profile and Client Connection Manager wizard" options, allows local users to execute arbitrary code by forcing an Explorer error. NOTE: a third-party researcher has stated that the options are "a convenience to users" and were not intended to restrict execution of arbitrary code.	unknown 2006-08-31	10.0	CVE-2006-4465 BUGTRAQ BUGTRAQ OTHER-REF
Nuked-Klan -- Nuked-Klan	Incomplete blacklist vulnerability in the nk_CSS function in nuked.php in Nuked-Klan 1.7 SP4.3 allows remote attackers to bypass anti-XSS features and inject arbitrary web script or HTML via JavaScript in an attribute value that is not in the blacklist, as demonstrated using the STYLE attribute of a B element.	unknown 2006-08-31	7.0	CVE-2006-4480 BUGTRAQ
NX5 -- NX5Linx	SQL injection vulnerability in NX5Linx 1.0 allows remote attackers to execute arbitrary SQL commands via the (1) c and (2) l parameters.	unknown 2006-08-31	7.0	CVE-2006-4504 OTHER-REF XF
NX5 -- NX5Linx	CRLF injection vulnerability in links.php in NX5Linx 1.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via a CRLF sequence in the url parameter.	unknown 2006-08-31	7.0	CVE-2006-4505 OTHER-REF
PHlyMail -- PHlyMail Lite	** DISPUTED ** PHP remote file inclusion vulnerability in handlers/email/mod.output.php in PHlyMail Lite 3.4.4 and earlier (Build 3.04.04) allows remote attackers to execute arbitrary PHP code via a URL in the _PM_[path][handler] parameter, a different vector than CVE-2006-4291. NOTE: This issue has been disputed by a third party, who states that the _IN_PHM_ declaration prevents this file from being called directly.	unknown 2006-08-28	7.0	CVE-2006-4429 BUGTRAQ BUGTRAQ
phpAlbum.net -- phpalbum	PHP remote file inclusion vulnerability in sommaire_admin.php in PhpAlbum (mod_phpalbum) 2.15 for PortailPHP allows remote attackers to execute arbitrary PHP code via a URL in the chemin parameter, a different vector than CVE-2006-3922.	unknown 2006-08-31	7.0	CVE-2006-4498 BUGTRAQ OTHER-REF BID XF
phpECard -- phpECard	PHP remote file inclusion vulnerability in functions.php in phpECard 2.1.4 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the include_path parameter.	unknown 2006-08-31	7.0	CVE-2006-4456 OTHER-REF BID FRSIRT SECUNIA XF
phpECard -- phpECard	PHP remote file inclusion vulnerability in index.php in phpECard 2.1.4 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the include_path parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-08-31	7.0	CVE-2006-4457 FRSIRT SECUNIA

ProManager -- ProManager	SQL injection vulnerability in note.php in ProManager 0.73 allows remote attackers to execute arbitrary SQL commands via the note_id parameter.	unknown 2006-08-28	7.0	CVE-2006-4419 OTHER-REF BID XF
SAP-DB -- SAP-DB MySQL -- MaxDB	Buffer overflow in SAP DB and MaxDB before 7.6.00.30 allows remote attackers to execute arbitrary code via a long database name when connecting via a WebDBM client.	unknown 2006-08-29	7.0	CVE-2006-4305 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Simple Machines -- Simple Machines Forum	Interpretation conflict in Simple Machines Forum (SMF) 1.1RCx before 1.1RC3, and 1.0.x before 1.0.8, does not properly unset variables when the input data includes a numeric parameter with a value matching an alphanumeric parameter's hash value, which allows remote attackers to perform directory traversal attacks to read arbitrary local files, lock topics, and possibly have other security impacts. NOTE: it could be argued that this vulnerability is due to a bug in the unset PHP command (CVE-2006-3017) and the proper fix should be in PHP; if so, then this should not be treated as a vulnerability in Simple Machines Forum.	unknown 2006-08-31	7.0	CVE-2006-4467 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF OTHER-REF
SQL-Ledger -- SQL-Ledger	Unspecified vulnerability in unspecified versions of SQL-Ledger allow remote attackers to gain access as any logged-in user via unknown vectors related to session handling.	unknown 2006-08-30	7.0	CVE-2006-4244 BUGTRAQ BID
Sun -- Solaris	pkgadd in Sun Solaris 10 before 20060825 installs files with insecure file and directory permissions (755 or 777) if the pkgmap file contains a "?" (question mark) in the mode field, which allows local users to modify arbitrary files or directories, a different vulnerability than CVE-2002-1871.	unknown 2006-08-29	7.0	CVE-2006-4439 SUNALERT SECUNIA FRSIRT OSVDB
Tor -- Tor	Unspecified vulnerability in Tor 0.1.0.x before 0.1.0.18 and 0.1.1.x before 0.1.1.23 allows remote attackers acting as an "entry node" within the Tor network to route arbitrary Tor traffic through clients or cause a denial of service (flood) via unspecified vectors.	unknown 2006-08-31	7.0	CVE-2006-4508 MLIST BID SECUNIA
Ultrize -- MiniBill	Multiple PHP remote file inclusion vulnerabilities in MiniBill 2006-07-14 (1.2.2) allow remote attackers to execute arbitrary PHP code via (1) a URL in the config[include_dir] parameter in actions/ipn.php or (2) an FTP path in the config[plugin_dir] parameter in include/initPlugins.php.	unknown 2006-08-31	7.0	CVE-2006-4489 OTHER-REF BID SECUNIA XF
VisualShapers -- ezContents	Multiple PHP remote file inclusion vulnerabilities in Visual Shapers ezContents 2.0.3 allow remote attackers to execute arbitrary PHP code via an empty GLOBALS[rootdp] parameter and an ftps URL in the (1) GLOBALS[admin_home] parameter in (a) diary/event_list.php, (b) gallery/gallery_summary.php, (c) guestbook/showguestbook.php, (d) links/showlinks.php, and (e) reviews/review_summary.php; and the (2) GLOBALS[language_home] parameter in (f) calendar/calendar.php, (g) news/shownews.php, (h) poll/showpoll.php, (i) search/search.php, (j) toprated/toprated.php, and (k) whatsnew/whatsnew.php.	unknown 2006-08-31	7.0	CVE-2006-4477 BUGTRAQ BID
VisualShapers -- ezContents	SQL injection vulnerability in headeruserdata.php in Visual Shapers ezContents 2.0.3 allows remote attackers to execute arbitrary SQL commands via the groupname parameter.	unknown 2006-08-31	7.0	CVE-2006-4478 BUGTRAQ BID
VisualShapers -- ezContents	Cross-site scripting (XSS) vulnerability in loginreq2.php in Visual Shapers ezContents 2.0.3 allows remote attackers to inject arbitrary web script or HTML via the subgroupname parameter.	unknown 2006-08-31	7.0	CVE-2006-4479 BUGTRAQ BID
Web3King -- Web3news	PHP remote file inclusion vulnerability in security/include/_class.security.php in Web3news 0.95 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the PHPSECURITYADMIN_PATH parameter.	unknown 2006-08-30	7.0	CVE-2006-4452 OTHER-REF BID SECUNIA FRSIRT OSVDB XF
XOOPS -- XOOPS	SQL injection vulnerability in edituser.php in Xoops before 2.0.15 allows remote attackers to execute arbitrary SQL commands via the user_avatar parameter.	unknown 2006-08-28	7.0	CVE-2006-4417 BUGTRAQ OTHER-REF OTHER-REF BID SECUNIA FRSIRT XF

Zend -- Zend Platform	Multiple buffer overflows in the (a) Session Clustering Daemon and the (b) mod_cluster module in the Zend Platform 2.2.1 and earlier allow remote attackes to cause a denial of service (crash) or execute arbitrary code via a (1) empty or (2) crafted PHP session identifier (PHPSESSID).	2006-08-21 2006-08-28	7.0	CVE-2006-4431 BUGTRAQ OTHER-REF FRSIRT SECUNIA FULLDISC BID OSVDB OSVDB XF
Ztml -- ezPortal/ztml CMS	SQL injection vulnerability in index.php in ezPortal/ztml CMS 1.0 allows remote attackers to execute arbitrary SQL commands via the (1) about, (2) album, (3) id, (4) use, (5) desc, (6) doc, (7) mname, (8) max, and possibly other parameters.	unknown 2006-08-31	7.0	CVE-2006-4501 BUGTRAQ BID
Ztml -- ezPortal/ztml CMS	ezPortal/ztml CMS 1.0 allows remote attackers to bypass authentication controls via a direct request to the "Administration Area" script.	unknown 2006-08-31	7.0	CVE-2006-4502 BUGTRAQ BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
AlberT -- AlberT-EasySite	PHP remote file inclusion vulnerability in AES/modules/auth/phpsecurityadmin/include/logout.php in AlberT-EasySite (AES) 1.0a5 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the PSA_PATH parameter.	unknown 2006-08-28	5.6	CVE-2006-4426 OTHER-REF BID SECUNIA FRSIRT
Clemens Wacha -- PHP iAddressBook	Cross-site scripting (XSS) vulnerability in PHP iAddressBook before 0.96 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2006-08-31	4.7	CVE-2006-4460 OTHER-REF
Cybozu -- Garoon	Multiple SQL injection vulnerabilities in Cybozu Garoon 2.1.0 for Windows allow remote authenticated users to execute arbitrary SQL commands via the (1) tid parameter in the (a) todo/view (aka TODO List View), (b) todo/modify (aka TODO List Modify), or (c) todo/delete functionality; the (2) pid parameter in the (d) workflow/view or (e) workflow/print functionality; the (3) uid parameter in the (f) schedule/user_view, (g) phonemessage/add, (h) phonemessage/history, or (i) schedule/view functionality; the (4) cid parameter in (j) todo/index; the (5) iid parameter in the (k) memo/view or (l) memo/print functionality; or the (6) event parameter in the (m) schedule/view functionality.	unknown 2006-08-29	4.2	CVE-2006-4444 OTHER-REF OTHER-REF BID SECUNIA
efiction -- efiction	index.php in eFiction before 2.0.7 allows remote attackers to bypass authentication and gain privileges by setting the (1) adminloggedin, (2) loggedin, and (3) level parameters to "1".	unknown 2006-08-28	5.6	CVE-2006-4427 OTHER-REF OTHER-REF BID SECUNIA FRSIRT OSVDB
Free Software Foundation Inc. -- phpGroupWare	Directory traversal vulnerability in calendar/inc/class.holidaycalc.inc.php in phpGroupWare 0.9.16.010 and earlier allows remote attackers to include arbitrary local files via a .. (dot dot) sequence and trailing null (%00) byte in the GLOBALS[phpgw_info][user][preferences][common][country] parameter.	unknown 2006-08-31	4.7	CVE-2006-4458 OTHER-REF BID FRSIRT SECUNIA XF
GNU -- GNU Debugger (GDB)	Buffer overflow in the (1) DWARF (dwarfread.c) and DWARF2 (dwarf2read.c) debugging code in GNU Debugger (GDB) 6.5 allows user-assisted attackers, or restricted users, to execute arbitrary code via a crafted file with a location block (DW_FORM_block) that contains a large number of operations.	unknown 2006-08-31	5.6	CVE-2006-4146 OTHER-REF
Interact Learning Community Environment -- Interact	Multiple PHP remote file inclusion vulnerabilities in interact 2.2, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) CONFIG[BASE_PATH] parameter in (a) admin/autoprompter.php and (b) includes/common.inc.php, and the (2) CONFIG[LANGUAGE_CPATH] parameter in (c) admin/autoprompter.php.	unknown 2006-08-29	5.6	CVE-2006-4448 BUGTRAQ OTHER-REF BID
iWebNegar -- iWebNegar	Cross-site scripting (XSS) vulnerability in comments.php in IwebNegar 1.1 allows remote attackers to inject arbitrary web script or HTML via the comment parameter.	unknown 2006-08-31	4.7	CVE-2006-4496 BUGTRAQ
iWebNegar -- iWebNegar	SQL injection vulnerability in comments.php in IwebNegar 1.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-08-31	4.7	CVE-2006-4497 BUGTRAQ BID

Jetstat.com -- JS ASP Faq Manager	SQL injection vulnerability in the administrator control panel in Jetstat.com JS ASP Faq Manager 1.10 allows remote attackers to execute arbitrary SQL commands via the pwd parameter (aka the Password field).	unknown 2006-08-31	4.7	CVE-2006-4463 BUGTRAQ
Joomla! -- Joomla!	Multiple unspecified vulnerabilities in Joomla! before 1.0.11, related to unvalidated input, allow attackers to have an unknown impact via unspecified vectors involving the (1) mosMail, (2) JosIsValidEmail, and (3) josSpoofValue functions; (4) the lack of inclusion of globals.php in administrator/index.php; (5) the Admin User Manager; and (6) the poll module.	unknown 2006-08-31	4.7	CVE-2006-4468 OTHER-REF
Joomla! -- Joomla!	Unspecified vulnerability in com_content in Joomla! before 1.0.11, when $mosConfig_hideEmail is set, allows attackers to perform the emailform and emailsend tasks.	unknown 2006-08-31	4.7	CVE-2006-4473 OTHER-REF
Microsoft -- Visual Studio	Microsoft Visual Studio 6.0 allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code by instantiating certain Visual Studio 6.0 ActiveX COM Objects in Internet Explorer, including (1) tcprops.dll, (2) fp30wec.dll, (3) mdt2db.dll, (4) mdt2qd.dll, and (5) vi30aut.dll.	unknown 2006-08-31	4.7	CVE-2006-4494 BUGTRAQ OTHER-REF BID
Microsoft -- Internet Explorer Microsoft -- Windows Server 2003	Microsoft Internet Explorer allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code by instantiating certain Windows 2000 ActiveX COM Objects including (1) ciodm.dll, (2) myinfo.dll, (3) msdxm.ocx, and (4) creator.dll.	unknown 2006-08-31	4.7	CVE-2006-4495 BUGTRAQ OTHER-REF BID
OpenBSD -- OpenBSD	isakmpd in OpenBSD 3.8, 3.9, and possibly earlier versions, creates Security Associations (SA) with a replay window of size 0 when isakmpd acts as a responder during SA negotiation, which allows remote attackers to replay IPSec packets and bypass the replay protection.	unknown 2006-08-28	4.7	CVE-2006-4436 OPENBSD OPENBSD BID SECTRACK SECUNIA OSVDB
Paessler -- IPCheck Server Monitor	Paessler IPCheck Server Monitor before 5.3.3.639/640 does not properly implement a "list of acceptable host IP addresses in the probe settings," which has unknown impact and attack vectors.	unknown 2006-08-31	4.9	CVE-2006-4461 OTHER-REF
PHP -- PHP	Multiple heap-based buffer overflows in the (1) str_repeat and (2) wordwrap functions in ext/standard/string.c in PHP before 5.1.5, when used on a 64-bit system, have unspecified impact and attack vectors, a different vulnerability than CVE-2006-1990.	unknown 2006-08-31	4.9	CVE-2006-4482 OTHER-REF OTHER-REF OTHER-REF SECUNIA
PHP -- PHP	The cURL extension files (1) ext/curl/interface.c and (2) ext/curl/streams.c in PHP before 5.1.5 permit the CURLOPT_FOLLOWLOCATION option when open_basedir or safe_mode is enabled, which allows attackers to perform unauthorized actions, possibly related to the realpath cache.	unknown 2006-08-31	4.7	CVE-2006-4483 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF SECUNIA
PHP -- PHP	The stripos function in PHP before 5.1.5 has unknown impact and attack vectors related to an out-of-bounds read.	unknown 2006-08-31	4.9	CVE-2006-4485 OTHER-REF SECUNIA
PHP -- PHP	Unspecified vulnerability in PHP before 5.1.6, when running on a 64-bit system, has unknown impact and attack vectors related to the memory_limit restriction.	unknown 2006-08-31	4.9	CVE-2006-4486 OTHER-REF OTHER-REF OTHER-REF SECUNIA
phpBB Group -- phpBB	usercp_avatar.php in PHPBB 2.0.20, when avatar uploading is enabled, allows remote attackers to use the server as a web proxy by submitting a URL to the avatarurl parameter, which is then used in an HTTP GET request.	unknown 2006-08-29	5.6	CVE-2006-4450 BUGTRAQ BID SECUNIA XF
phpCOIN -- phpCOIN	PHP remote file inclusion vulnerability in coin_includes/constants.php in phpCOIN 1.2.3 allows remote attackers to execute arbitrary PHP code via the _CCFG[_PKG_PATH_INCL] parameter.	unknown 2006-08-28	5.6	CVE-2006-4424 OTHER-REF BID FRSIRT SECUNIA XF
phpCOIN -- phpCOIN	Multiple PHP remote file inclusion vulnerabilities in phpCOIN 1.2.3 allow remote attackers to execute arbitrary PHP code via the _CCFG[_PKG_PATH_INCL] parameter in coin_includes scripts including (1) api.php, (2) common.php, (3) core.php, (4) custom.php, (5) db.php, (6) redirect.php or (7) session_set.php. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-08-28	5.6	CVE-2006-4425 FRSIRT SECUNIA XF OSVDB OSVDB OSVDB OSVDB

				OSVDB OSVDB
Sony -- PlaystationPortable	Unspecified vulnerability in the TIFF viewer (possibly libTIFF) in the Photo Viewer in the Sony PlaystationPortable (PSP) 2.00 through 2.80 allows local users to execute arbitrary code via crafted TIFF images. NOTE: due to lack of details, it is not clear whether this is related to other issues such as CVE-2006-3464 or CVE-2006-3465.	unknown 2006-08-31	4.9	CVE-2006-4507 OTHER-REF FRSIRT SECUNIA
X.org -- xload X.org -- xterm X.org -- X11R6 X.org -- xorg-server X.org -- xdm X.org -- xf86dga X.org -- xinit X.org -- emu-linux-x87-xlibs X.org -- X11R7	X.Org and XFree86, including libX11, xdm, xf86dga, xinit, xload, xtrans, and xterm, does not check the return values for setuid and seteuid calls when attempting to drop privileges, which might allow local users to gain privileges by causing those calls to fail, such as by exceeding a ulimit.	unknown 2006-08-29	4.9	CVE-2006-4447 MLIST GENTOO BID SECUNIA SECUNIA
Ztml -- ezPortal/ztml CMS	Cross-site scripting (XSS) vulnerability in index.php in ezPortal/ztml CMS 1.0 allows remote attackers to inject arbitrary web script or HTML via the (1) about, (2) again, (3) lastname, (4) email, (5) password, (6) album, (7) id, (8) table, (9) desc, (10) doc, (11) mname, (12) max, (13) htpl, (14) pheader, and possibly other parameters.	unknown 2006-08-31	4.7	CVE-2006-4500 BUGTRAQ BID

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Cisco -- Network Admission Control Cisco -- Cisco Clean Access	The Cisco Network Admission Control (NAC) 3.6.4.1 and earlier allows remote attackers to prevent installation of the Cisco Clean Access (CCA) Agent and bypass local and remote protection mechanisms by modifying (1) the HTTP User-Agent header or (2) the behavior of the TCP/IP stack. NOTE: the vendor has disputed the severity of this issue, stating that users cannot bypass authentication mechanisms.	2006-08-12 2006-08-28	2.3	CVE-2006-4430 BUGTRAQ BUGTRAQ BUGTRAQ CISCO BID BUGTRAQ
Clemens Wacha -- PHP iAddressBook	Cross-site scripting (XSS) vulnerability in PHP iAddressBook before 0.95 allows remote attackers to inject arbitrary web script or HTML via the cat_name parameter, related to adding a category. (categories field). NOTE: some details are obtained from third party information.	unknown 2006-08-29	2.3	CVE-2006-4442 OTHER-REF BID FRSIRT OSVDB SECUNIA
Cybozu -- Cybozu Pocket Cybozu -- Garoon 1 Cybozu -- Cybozu AG Cybozu -- Collaborex Cybozu -- Mailwise	Directory traversal vulnerability in Cybozu Collaborex, AG before 1.2(1.5), AG Pocket before 5.2(0.8), Mailwise before 3.0(0.3), and Garoon 1 before 1.5(4.1) allows remote authenticated users to read arbitrary files via unspecified vectors.	unknown 2006-08-31	2.3	CVE-2006-4491 OTHER-REF OTHER-REF OTHER-REF SECTRACK SECUNIA SECUNIA
Cybozu -- Cybozu Office	Unspecified vulnerability in Cybozu Office 6.5 Build 1.2 for Windows allows remote attackers to obtain sensitive information, including users and groups, via unspecified vectors.	unknown 2006-08-31	2.3	CVE-2006-4492 OTHER-REF OTHER-REF SECUNIA
Cybozu Corporation -- Share 360 Cybozu Corporation -- Cybozu Office	Multiple directory traversal vulnerabilities in Cybozu Office before 6.6 Build 1.3 and Share 360 before 2.5 Build 0.3 allow remote authenticated users to read arbitrary files via a .. (dot dot) sequence via the id parameter in (1) scripts/cbag/ag.exe or (2) scripts/s360v2/s360.exe.	unknown 2006-08-31	2.3	CVE-2006-4490 OTHER-REF OTHER-REF OTHER-REF OTHER-REF SECTRACK SECUNIA SECUNIA XF
DUware -- DUpoll	DUware DUpoll 3.0 and 3.1 stores _private/Dupoll.mdb under the web document root with insufficient access control, which allows remote attackers to obtain sensitive information such as usernames and passwords.	unknown 2006-08-31	2.3	CVE-2006-4487 BUGTRAQ SECUNIA
HLstats -- HLstats	Cross-site scripting (XSS) vulnerability in hlstats.php in HLstats 1.34 allows remote attackers to inject arbitrary web script or HTML via the q parameter.	unknown 2006-08-30	2.3	CVE-2006-4454 FULLDISC BID OSVDB SECUNIA XF

Joomla! -- Joomla!	Interpretation conflict in Joomla! before 1.0.11 does not properly unset variables when the input data includes a numeric parameter with a value matching an alphanumeric parameter's hash value, which allows remote attackers to have an unspecified impact. NOTE: it could be argued that this vulnerability is due to a bug in the unset PHP command (CVE-2006-3017) and the proper fix should be in PHP; if so, then this should not be treated as a vulnerability in Joomla!.	unknown 2006-08-31	2.3	CVE-2006-4466 OTHER-REF
Joomla! -- Joomla!	Multiple unspecified vulnerabilities in Joomla! before 1.0.11, related to "Injection Flaws," allow attackers to have an unknown impact via (1) globals.php, which uses include_once() instead of require(); (2) the $options variable; (3) Admin Upload Image; (4) ->load(); (5) content submissions when frontpage is selected; (6) the mosPageNav constructor; (7) saveOrder functions; (8) the absence of "exploit blocking rules" in htaccess; and (9) the ACL.	unknown 2006-08-31	2.3	CVE-2006-4476 OTHER-REF
Microsoft -- Internet Explorer	Heap-based buffer overflow in DirectAnimation.PathControl COM object (daxctle.ocx) in Microsoft Internet Explorer 6.0 SP1 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a Spline function call whose first argument specifies a large number of points.	unknown 2006-08-29	2.3	CVE-2006-4446 BUGTRAQ OTHER-REF BID SECTRACK XF
ModernGigabyte -- ModernBill	ModernBill 5.0.4 and earlier uses cURL with insecure settings for CURLOPT_SSL_VERIFYPEER and CURLOPT_SSL_VERIFYHOST that do not verify SSL certificates, which allows remote attackers to read network traffic via a man-in-the-middle (MITM) attack.	unknown 2006-08-31	2.3	CVE-2006-4499 OTHER-REF SECUNIA
MyBB -- MyBB	Cross-site scripting (XSS) vulnerability in attachment.php in MyBulletinBoard (MyBB) 1.1.7 and possibly other versions allows remote attackers to inject arbitrary web script or HTML via a GIF image that contains URL-encoded Javascript, which is rendered by Internet Explorer.	unknown 2006-08-29	2.3	CVE-2006-4449 BUGTRAQ BID SECUNIA XF
Nokia -- Nokia Symbian 60 Browser	The Nokia Browser, possibly Nokia Symbian 60 Browser 3rd edition, allows remote attackers to cause a denial of service (crash) via JavaScript that constructs a large Unicode string.	unknown 2006-08-31	2.3	CVE-2006-4464 BUGTRAQ OTHER-REF BID
Novell -- Novell Identity Manager	idmlib.sh in nxdrv in Novell Identity Manager (IDM) 3.0.1 allows local users to execute arbitrary commands via unspecified vectors, possibly involving the " (quote) and \ (backslash) characters and eval injection.	unknown 2006-08-31	3.3	CVE-2006-4506 OTHER-REF BID SECTRACK
NX5 -- NX5Linx	Directory traversal vulnerability in link.php in NX5Linx 1.0 allows remote attackers to read arbitrary files via the logo parameter.	unknown 2006-08-31	2.3	CVE-2006-4503 OTHER-REF XF
OpenBSD -- OpenBSD	OpenBSD 3.8, 3.9, and possibly earlier versions allows context-dependent attackers to cause a denial of service (kernel panic) by allocating more semaphores than the default.	unknown 2006-08-28	3.3	CVE-2006-4435 OPENBSD OPENBSD BID SECTRACK SECUNIA OSVDB
Phaos -- Phaos	Directory traversal vulnerability in include_lang.php in Phaos 0.9.2 allows remote attackers to include arbitrary local files via ".." sequences in the lang parameter.	unknown 2006-08-28	2.3	CVE-2006-4420 OTHER-REF BID XF
PHP -- PHP	PHP before 4.4.3 and 5.x before 5.1.4 does not limit the character set of the session identifier (PHPSESSID) for third party session handlers, which might make it easier for remote attackers to exploit other vulnerabilities by inserting PHP code into the PHPSESSID, which is stored in the session file. NOTE: it could be argued that this not a vulnerability in PHP itself, rather a design limitation that enables certain attacks against session handlers that do not account for this limitation.	2006-08-21 2006-08-28	2.3	CVE-2006-4433 BUGTRAQ OTHER-REF FRSIRT SECUNIA
PHP -- PHP	The (1) file_exists and (2) imap_reopen functions in PHP before 5.1.5 do not check for the safe_mode and open_basedir settings, which allows local users to bypass the settings. NOTE: the error_log function is covered by CVE-2006-3011, and the imap_open function is covered by CVE-2006-1017.	unknown 2006-08-31	1.6	CVE-2006-4481 OTHER-REF SECUNIA
PHP -- PHP	Buffer overflow in the LWZReadByte_ function in ext/gd/libgd/gd_gif_in.c in the GD extension in PHP before 5.1.5 allows remote attackers to have an unknown impact via a GIF file with input_code_size greater than MAX_LWZ_BITS, which triggers an overflow when initializing the table array.	unknown 2006-08-31	1.9	CVE-2006-4484 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF SECUNIA

PmWiki -- PmWiki	Cross-site scripting (XSS) vulnerability in PmWiki before 2.1.18 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving "table markups".	unknown 2006-08-30	2.3	CVE-2006-4453 OTHER-REF BID SECUNIA
Sendmail Consortium -- Sendmail	Use-after-free vulnerability in Sendmail before 8.13.8 allows remote attackers to cause a denial of service (crash) via a long "header line", which causes a previously freed variable to be referenced. NOTE: the original developer has disputed the severity of this issue, saying "The only denial of service that is possible here is to fill up the disk with core dumps if the OS actually generates different core dumps (which is unlikely)... the bug is in the shutdown code (finis()) which leads directly to exit(3), i.e., the process would terminate anyway, no mail delivery or receiption is affected."	unknown 2006-08-28	2.3	CVE-2006-4434 OTHER-REF OPENBSD OPENBSD BID SECTRACK SECUNIA SECUNIA DEBIAN MANDRIVA MLIST SECUNIA SECUNIA
WikePage -- WikePage	Directory traversal vulnerability in index.php for Wikepage 2006.2a Opus 10 allows remote attackers to include arbitrary local files via the lng parameter, as demonstrated by inserting PHP code into a log file.	unknown 2006-08-28	3.7	CVE-2006-4418 OTHER-REF BID FRSIRT SECUNIA XF
xbiff2 -- xbiff2	xbiff2 1.9 creates $HOME/.xbiff2rc in a user's home directory with insecure file permissions, which allows local users to obtain sensitive information such as login credentials. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-08-31	1.6	CVE-2006-4493 BID SECUNIA
XChat -- XChat	** DISPUTED ** Unspecified vulnerability in Xchat 2.6.7 and earlier allows remote attackers to cause a denial of service (crash) via unspecified vectors involving the PRIVMSG command. NOTE: the vendor has disputed this vulnerability, stating that it does not affect 2.6.7 "or any recent version".	unknown 2006-08-30	2.3	CVE-2006-4455 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID SECTRACK XF
YaPiG -- YaPiG	Cross-site scripting (XSS) vulnerability in template/default/thanks_comment.php in Yet Another PHP Image Gallery (YaPIG) 0.95b allows remote attackers to inject arbitrary web script or HTML via the D_REFRESH_URL parameter.	unknown 2006-08-28	2.3	CVE-2006-4421 BUGTRAQ
Zend -- Zend Platform	Directory traversal vulnerability in Zend Platform 2.2.1 and earlier allows remote attackes to overwrite arbitrary files via a .. (dot dot) sequence in the final component of the PHP session identifier (PHPSESSID). NOTE: in some cases, this issue can be leveraged to perform direct static code injection.	2006-08-21 2006-08-28	2.3	CVE-2006-4432 BUGTRAQ OTHER-REF FRSIRT SECUNIA OSVDB

Back to top